UoS Information Security

ICT Acceptable Use Policy

Doc ID: UoS-IS-Doc201-ICT Acceptable Use Policy-2020

Version Number 5.0

March 24th, 2020

Author(s):
Head of Information Security, Digital Strategy Office, Digital IT

Classification: Public

Table of Contents

1. Document Introduction

The ICT Acceptable Use Policy (ICT AUP) defines a common set of rules and behaviours relating to the University of Salford's IT infrastructure and other information assets.

The policy addresses the need to protect the University and its users' data, balanced with the need to protect the rights of the students, employees, associates, and alumni.

This policy is a component of 2 University of Salford Frameworks:

- The University Information Framework, which states that all those who are authorised to, should be able to easily access all the information they need to fulfil their role.

- The UoS Information Security Framework, which defines procedures and standards around Information Security. More specifically, this document promotes understanding and gathers consents consent of/to some of the security measures defined in the framework.

The ICT Acceptable Use Policy applies to all authorised users of the University's ICT facilities encompassing; students, alumni, employees and associates (including contractors and service providers) of the University. Any individual accessing University information using the ICT facilities, whether on personally owned or University issued devices, is deemed to have accepted this Policy and is bound by its terms.

This policy does not form part of the contract of employment or student contract and can therefore be amended without users' consent. The University may make changes to the Policy at any time. Users will be notified of the change via email sent to their University of Salford email address. Parties without access to University email account should regularly, at least quarterly, review the policies section of the www.salford.ac.uk website to check for any changes to this document.

2. Fundamental Principles

2.1. All Users

All users of the ICT facilities must comply with the following principles around responsible and courteous use of the ICT facilities:

1. This policy and policies that are applied by bodies external to the University in respect of the ICT facilities, including but not restricted to JANET (Joint Academic Network) and, with respect to Microsoft 365 email and collaboration platforms, Microsoft Corporation.

2. All relevant copyright legislation, licences and agreements for software and electronic information resources.

3. All applicable laws in the United Kingdom.

2.2. System Owners

System owners shall ensure their information systems or supporting infrastructure adhere to UoS IT & Information Security guidelines (and/or industry best practice where such guidelines are missing) for matters regarding technical security measures and system governance.

2.3. Reporting Problems & Requests

Any technical problems, requests, or concerns regarding a suspected policy breach should be reported directly to the Digital IT Service Desk.

3. Policy Exceptions

Where (for operational, research, or academic reasons) an exception to this Policy is required, the request should be made in writing to the University's ITSERT Team (itsert@salford.ac.uk) and approved by a relevant member of the University Management Team. We recommend first contacting the Digital IT Service Desk in case solutions that may meet your requirements are already in place.

4. ICT Facilities

4.1. Definition

In this document, the term "ICT facilities" encompasses (but is not restricted to) the following services and equipment provided by the University of Salford and third parties on its behalf to access and process University information:

1. Network infrastructure and services, including (but not limited to) the physical infrastructure (whether cable or wireless), together with servers, firewalls, connection points, switches and routers, internet services, email, messaging, shared file stores, printing, telephony and fax services, CCTV, and digital physical access controls.

2. University owned computing hardware (hereafter referred to as devices), both fixed and portable, including (but not exclusively) workstations, laptops, tablets, smartphones, servers, printers, scanners, and monitors;

3. Software, databases, any structured or unstructured University data, applications, information systems & services (including those hosted by 3rd parties), virtual learning and videoconferencing platforms, ICT laboratories, electronic journals & e-books.

4.2. Reasonable Personal Use

ICT facilities are provided to users for University business purposes to support teaching, learning, research, professional, and administrative activities.

Occasional and reasonable personal use of the facilities is acceptable; however, University business purposes of ICT facilities take priority over any personal use. Users shall ensure personal use is occasional, reasonable and ensure personal use is compatible with and does not contravene the primary purpose of the facilities; interfere with, conflict with or take priority over the performance of University duties; waste resources; deny or impair the service to other users or have a negative impact on the University, its reputation, or other users.

4.3. Third Party Access

Staff members' work communications, files, and data may need to be accessed during their absence. Any such access will only be granted in accordance with the *Third-Party Access to IT Account Form* which can be obtained through the Service Portal. The same process may be applied for authorised investigations.

4.4. Discretional Access

The ICT facilities available and access to University information will vary based on user group, job role, and other considerations.

The University ultimately reserves the right to refuse access to particular computing resources where it considers that there is a security risk to its information or ICT facilities.

4.5. Liability of Use

The University does not endorse any third-party goods or services unless specifically indicated and is not responsible for any goods or services that are accessible via third party websites;

The University provides the ICT facilities for the benefit of itself and its staff, students and alumni and no guarantee is given that use of the ICT facilities will be fault-free, uninterrupted and secure.

Users will be solely responsible for all claims, liabilities, damages, costs and expenses suffered or incurred by the University as a result of said users' use of the ICT facilities in contravention of this policy, or through any other form of bad faith on their part.

Users of the ICT facilities understand and agree that the University shall not be held liable for any loss connected with their use of the ICT facilities however that loss may arise, including but not limited to loss that is caused by unintended negligence on the part of the University.

5. Email, Communication, Data Classification.

Users shall ensure personal use of email and other collaboration tools is occasional, reasonable and ensure personal use is compatible with and does not contravene the primary purpose of the facilities; interfere with, conflict with or take priority over the performance of University duties; waste resources; deny or impair the service to other users or have a negative impact on the University or other users.

5.1. Staff & Associate Email

When provided, University of Salford email accounts should be used as the primary mechanism for email communication with the University and for University duties by staff and associates.

5.2. Student Email

Students should endeavour to use their university email addresses whenever possible for any university function. Any non-automated requests for services or support through the help desk should be performed via University email or over the phone with the Service Desk.

5.3. Alumni Email

The provision of an Email for Life account for each alumnus is at the discretion of the University, where provided, is subject to the following:

1. Alumni *Email for Life* accounts may be terminated immediately at any time without prior notice if the University believes or suspects that alumni have contravened this Policy in any way or that its ICT facilities have been or will be put at risk.

2. Email for Life accounts may also be terminated if they have not been accessed for 90 or more days (or any shorter period which the University may notify to alumni).

3. The contents of Email for Life accounts that are terminated will be irretrievably deleted. The University will not be held liable for any alleged loss of alumni data resulting from such deletion.

5.4. Other Communication

Other methods of communication should be limited to those provided and supported by the University. These include but are not limited to Microsoft Teams, Yammer, and other

collaboration and communication platforms. For programmes of study, the Blackboard / Virtual Learning Environment is the alternative University provided communication mechanism.

Other platforms should only be used with an explicit approval from UoS Information Security through a risk/policy exemption request.

5.5. Data Classification

All users are expected to understand the data classification of the document(s) they are handling and must not place that information at risk; whether accidentally or deliberately. Such risks may include sending document(s) to a commercial competitor, a member of the public, a colleague or applying insufficient safeguards to the information in electronic or paper form so that it could be exposed to unintended individuals. A Data Classification Guide can be obtained from Information Governance via the Service Portal.

6. Protecting University Information and ICT Facilities

6.1. Protective Measures

The University needs to protect its ICT facilities, data, including the personal data of its employees, students and others whose data it manages, reputation and business.

Underpinning this need is the University's ability to take the following protective measures, to which those subject to this AUP consent:

1. The presence of host-based software agents on University systems that monitor and protect systems, data, and users from malware and malicious activity.

2. Network Monitoring to detect malicious activity.

3. The implementation of Multi-Factor Authentication (MFA) which may require, by the user, the installation of an application or receipt of a message on a personal device (typically a phone) to confirm the user's identity when a potentially unauthorised access to an account is detected. This is in order to protect potentially compromised account credentials from being misused.

4. Access controls around removable media to prevent the spread of malware or the theft of data through USB keys and other removable media. Various levels of flexibility may be assigned depending on your job or academic requirements, but these should not be exceeded without authorisation. Contact the Digital IT Service Desk for more details. Users shall not attempt to otherwise circumvent these controls.

5. The blocking of unauthorised communication, file sharing, and other sites and/or protocols. If such restrictions are conflicting with a user's work or study requirements, the user may contact the Digital IT Service Desk for a possible exemption. Users shall not attempt to otherwise circumvent these controls.

6. Unless specifically authorised, users are not to have local administrative privileges on their issued systems in order to prevent malicious activity and unauthorised installation of software which can then expose the University to significant risks.

   Users can request a utility that grants temporary administrative access provided they provide a compelling business case, abide by the utility's corresponding Acceptable Use Policy, agree to all use of the utility be monitored, and limit their use of the utility to those needs outlined in their business case justification.

7. Users consent to the fact that under certain circumstances, for investigative or business continuity reasons, access to their accounts may be granted to relevant staff under approval of the Information Governance department.

6.2. User Responsibilities

Users agree to the following responsibilities:

1. Be responsible for their University ICT accounts and not share access or credentials to these accounts.

2. To lock their computer's screen using the CTRL-ALT-DEL or WINDOWS-L key combinations whenever it is left unattended. University computer accounts must not be left unlocked, logged-in, and/or unattended in a way that risks access to the account, system, or information displayed on screen by an unauthorised user.

3. Wherever possible, follow Digital IT password complexity standards on any system that supports them.

4. Be mindful of the effect on University (and personal) reputation in relation to any use of social media whether personal or work related. Social media leaves a permanent record and electronic footprint. Using social media in such a way as to bring the University into disrepute will be actionable as a disciplinary matter.

5. Ensure personally owned devices being used for university functions or with connectivity to University ICT facilities have up to date and patched operating systems and active anti-virus protection.

6. Not open or run files received in an unsolicited manner (whether by email or some other method).

7. Be vigilant with regards to phishing emails requesting credentials or other information. Note that phishing emails may direct you to very authentic-looking websites such as the Microsoft 365 portal. Validate when in doubt.

8. Notify the Digital IT Service Desk of University IT equipment changes related to office moves, or role changes, or any other reason). This helps ensure the IT Equipment register stays up to date.

9. Return all University IT equipment to Digital IT at the end of employment, contract, or use period. This ensures not just recovery of the asset but that any sensitive data is appropriately handled and/or erased. It also ensures the asset is properly reimaged where applicable.

10. Ensure that all university information including personal data has been deleted from personally owned devices at the end of employment.

11. Obtain written approval from relevant Data Owners and System Owners before transmitting University confidential information externally.

12. Ensure data is adequately protected in storage and transit (including use of encryption where appropriate) Contact the Service Desk for applicable standards.

13. Employees and associates shall ensure they take the necessary precautions when working from remote / off campus locations and processing University data, including but not limited to:

    a. Being aware that using personally owned mobile devices to carry out University work can create risks including, data protection issues, vulnerability to virus infection or malware, and unintentional or unlawful compromise of data.

    b. Where possible, use University issued computers/devices to access and process University information from remote locations. Ensure equivalent protections are in place when non-University devices are used.

    c. Use only University provided or approved storage (on-premise shared drives and cloud storage) to store University data.

    d. Ensure University information is stored securely if extracted from University managed storage and/or systems: Obtain System Owner and Data Owner authorisation and use an encrypted USB / mobile device. Ensure it is the minimum information necessary; is temporary and is deleted as soon as the information is no longer required.

    e. Do not store University information in cloud storage facilities not specifically approved by the University (Digital IT). This typically means using the University's Microsoft 365 services. Instances of prohibited storage include personal drives such as Google drive, Dropbox, iCloud, etc.

    f. Do not transfer University information through file transfer facilities not specifically approved by the University (Digital IT). This typically means using the University's

Microsoft 365 services. Instances of prohibited file transfer facilities include WeTransfer, TransferNow, WeSendit, etc.

g. Irreversibly delete University information from any personally owned IT equipment before leaving University employment or when selling, transferring or disposing of the device. Note that simply deleting files typically does not render them unrecoverable. Contact Digital IT for advice on thoroughly deleting or sanitising data/drives. You will be held liable for any University data leaked through your personal device.

h. Use reasonable care and security measures to prevent loss or theft of IT equipment and information. Do not leave IT equipment unattended in a public area or when travelling, keep it in a secure access-controlled area when not in use, and avoid leaving sensitive information on your desk. Personal devices should have access controls (Passwords, PIN codes, biometrics, etc.) similar to those on University (Digital IT) issued devices.

i. Report loss/theft/breach of University information or IT equipment to the Digital IT Service Desk immediately. The Service desk will advise on appropriate actions including: password change, user notification to network provider; remote wiping of device, IT asset register update, security incident investigation, and asset replacement process.

j. Report theft or loss of University IT equipment to the Service Desk who will in turn report it to the Police and/or to the Estates Security team as appropriate.

7. Prohibited ICT Activity

The following items are strictly prohibited and subject to immediate disciplinary action. Users may not:

1. Cause the good name & reputation of the University or any part of it to be damaged or undermined by carrying out, facilitating or furthering inappropriate, criminal or any other activity that conflicts with all applicable laws in the United Kingdom and / or University policy or regulations.

2. Contravene regulations and policies applied by bodies external to the University in respect of the ICT facilities, including but not restricted to JANET (Joint Academic Network) and Microsoft Corporation.

3. Sell, redistribute, repurpose, or dispose of any part of the ICT facilities, including but not limited to: software, hardware, licenses, or any other item or data belonging to the University without explicit authorisation and only if doing so is part of the individual's job role.

4. Commit the University via any means to any contract, binding agreement, or any other form of obligation (except for staff who are expressly authorised to do so using University procedures).

5. Carry out activities of a nature that compete with the University's business or other interests or obtain unauthorised commercial gain from University resources.

6. Use university resources (compute, network, power, etc.) for crypto-mining (e.g. Bitcoin mining) or other resource-intensive activities without authorisation.

7. Carry out activities that conflict with an employee's obligations to the University as their employer.

8. Carry out activities that unreasonably waste network or computing resources, deny ICT facilities to authorised users, or continue to carry out activity after a designated Digital IT authority has requested that use ceases.

9. Deliberately or intentionally receive, access, create, change, store, download, upload, share, use, transmit, or otherwise facilitate:

    a) Any terrorist related or extremist material, or any data capable of being resolved into such material as per the University's Prevent Duty under s26(1) of the Counter-Terrorism and Security Act 2015 as specified by guidance issued under s29(1) of the Act. Anyone witnessing such material should report it to University authorities. (See section 3 for exceptions around teaching and/or research purposes.)

    b) Any illegal, obscene or indecent images, data or other material, or any data capable of being resolved into such material. Anyone witnessing such material should report it to University authorities. (See section 3 for exceptions around teaching and/or research purposes.)

    c) Any infected material or malicious code (including, but not restricted to, computer viruses, spyware, trojan horses and worms), whether designed specifically or not, to be destructive to the correct functioning of computer systems, software, networks, data storage and others' data, or attempt to circumvent any precautions taken or prescribed to prevent such damage.

    d) Any material which discriminates or encourages discrimination on any grounds. (See section 3 for exceptions around teaching and/or research purposes.)

    e) Any material which the University may deem to be advocating, inciting or encouraging illegal activity, threatening, harassing, defamatory, bullying or disparaging of others, abusive, libellous, slanderous, indecent, obscene, deliberately causing offense, annoyance, inconvenience or needless anxiety. (See section 3 for exceptions around teaching and/or research purposes.)

    f) Any material that infringes the copyright or confidentiality of another person or institution, or infringes the copyright laws of the UK and/or other countries (including but not exclusive to music, films, radio and TV); place links to websites which have links to, or display, pornographic or inappropriate material, or which facilitate illegal or

improper use, or place links to bulletin boards which are likely to publish defamatory materials or discriminatory statements; or where copyright protected works such as computer software, films, games or music are unlawfully distributed.

10. Falsify emails to make them appear to have originated from someone else or send anonymous messages without clear indication of the sender.

11. Carry out activities that criticise or harm individuals or that violate the privacy of other individuals.

12. Use file-sharing or other systems to download or upload copyright material without the copyright owner's permission (including but not limited to music, films, games, and software).

13. Deliberately or unintentionally attempt to circumvent the University's ICT facility controls and policies through VPNs, TOR, or any other technical or non-technical method.

14. Access any University system by circumventing the network authentication process, gain or attempt to gain unauthorised access to facilities or services via the University ICT facilities, using automated processes or otherwise.

15. Allow, incite, encourage or enable others to gain or attempt to gain unauthorised access to, or carry out unauthorised modification to the University's or others' ICT facilities; overload, change, damage, curtail, corrupt, disrupt, deny, modify, re-route, dismantle or destroy (or cause to be overloaded, changed, damaged, curtailed, corrupted, disrupted, denied, modified, re-routed, dismantled, or destroyed) any ICT facility, network component, equipment, software or data, or its functions or settings, which is the property of the University, its Users, visitors, suppliers or anyone else, without the express written permission of the University's Chief Information Officer.

16. Connect any non-approved or personally owned ICT equipment to the University physical (wired) network points without written authorisation of Digital IT Services (via the Digital IT Service Desk).

17. Intentionally or unintentionally transmit unsolicited or unauthorised commercial or advertising material within the University or to other individuals or organisations in contravention of the University privacy statement or use any portion of the ICT facilities as a destination linked from such material. Such material includes unsolicited e-mail (spam), chain letters, hoax virus warnings, pyramid letters or other junk mail of any kind.

18. Make, use, install, possess, distribute, sell, hire or otherwise deal with any unauthorised copies of software for any purpose without the licence and permission of its owner.

19. Install any software without authorisation of Digital IT (via Digital IT Service Desk).

20. Save or share any University owned confidential information on any cloud computing service unless it is under a University negotiated contract approved by Digital IT Services and by Legal & Governance Directorate.

21. Otherwise transmit, distribute, discuss or disclose (on Message Boards, email or any other mechanism) any University owned or held confidential information, including personal data without the University's permission (See Related Documentation).

8. Policy Enforcement

Breaches of the ICT Acceptable Use Policy may be investigated by the IT Security Emergency Response Team (ITSERT) or relevant School or Professional Service in line with the appropriate University disciplinary policy. The initiating School or Professional Service will be responsible for communications with the subject and should make it clear to the subject under which policy action is being taken. Sanctions for violations of the ICT AUP may include:

1. Suspension or withdrawal of University ICT facilities.

2. Disconnection, seizure & inspection of any ICT equipment that is in violation of this policy.

3. Initiation of disciplinary action in accordance with the applicable discipline policy. In the case of staff, this could lead to a disciplinary sanction up to and including dismissal. In the case of students, this could lead to a disciplinary sanction including expulsion.

4. Where there is evidence of a criminal offence, the issue will be reported to the Police. The University will co-operate with and disclose copies of any data and ICT activity logs, and equipment used to the Police (or other appropriate external agencies).

9. Agreement

Please sign the below agreement and return the signed page to University of Salford Human Resources Directorate. Please retain a copy of the policy for your future reference.

The undersigned confirms to have read, understood the ICT Acceptable Use Policy V5.0 and agrees to abide by its terms and the possible disciplinary action(s) listed should they violate said policy.

Name (in block letters):	
Signature:	
Date (DD-MM-YYYY):	

It is strongly suggested to keep a copy of the latest ICT Acceptable Use Policy for personal reference.